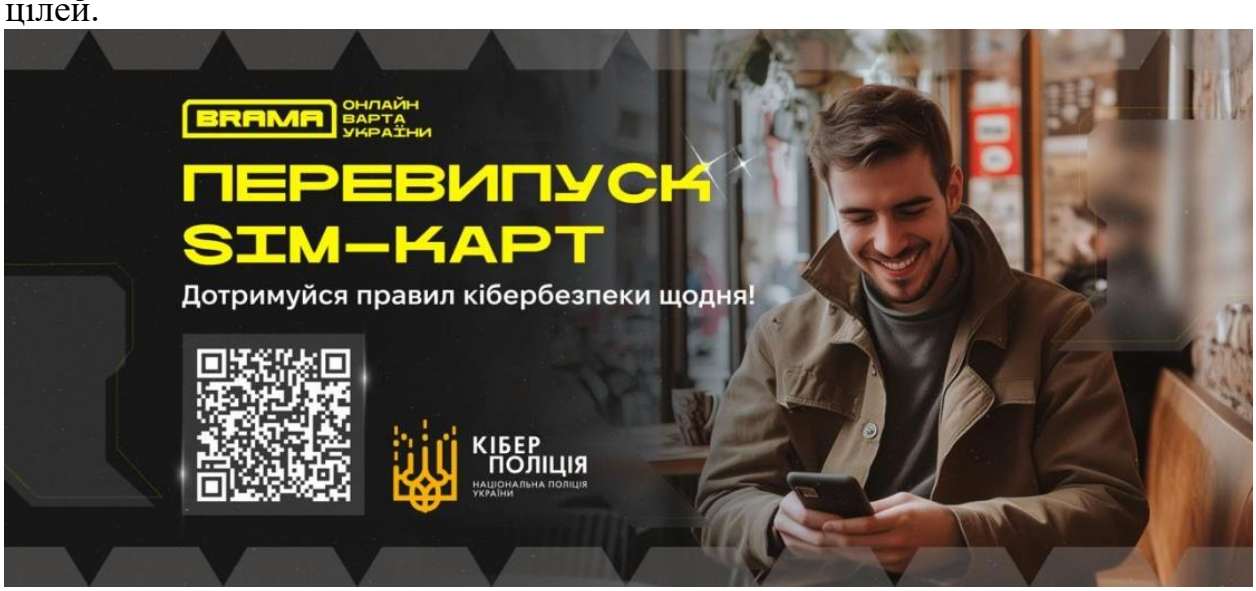
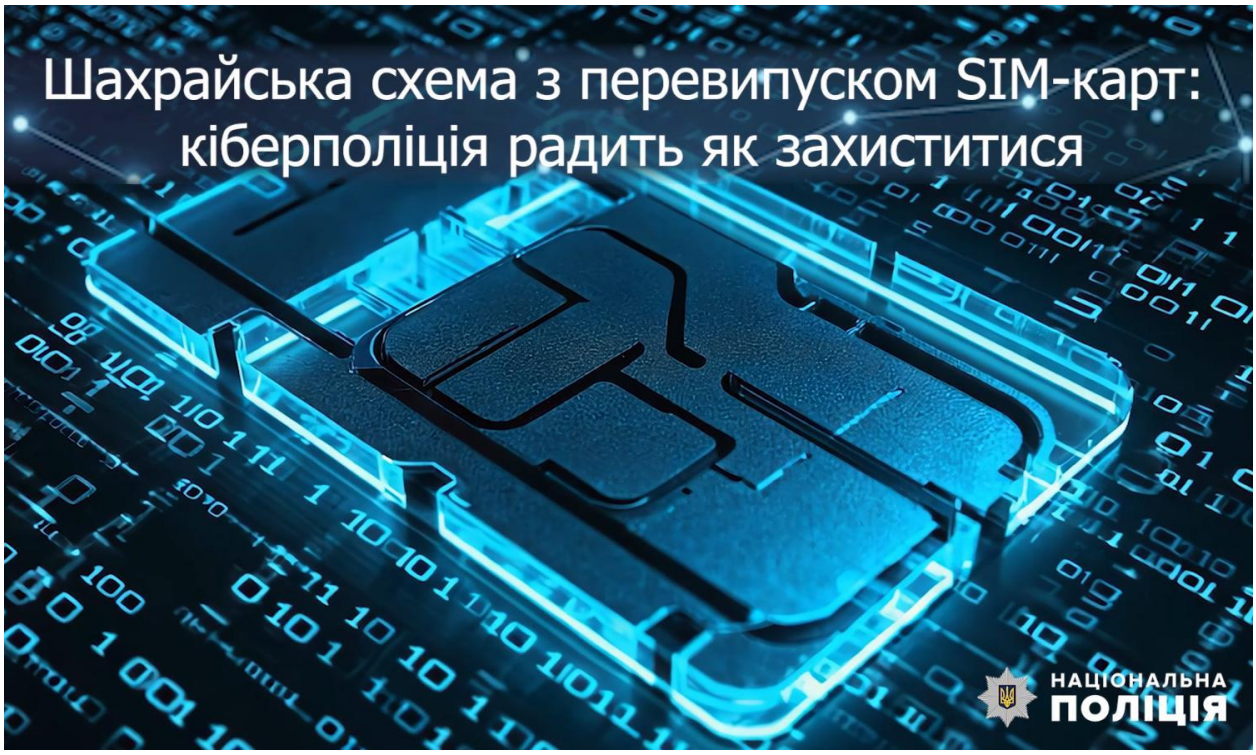
Перевипуск SIM-карт

Одна з небезпечних злочинних махінацій – перевипуск sim-картки без відома власника. Отримавши контроль над вашим номером, зловмисники можуть отримати доступ до банківських рахунків, оформити кредити на ваше ім’я, а також зламати електронні облікові записи та використати їх для зловмисних цілей.





Таким чином, втрата власної sim-картки – це не лише побутові незручності, а й серйозна загроза фінансовій безпеці та приватності громадян. Тому важливо

знати, як протидіяти таким атакам і які кроки здійснити у разі підозри на зловмисні дії.

Шахраї використовують методи соціальної інженерії, фішингові сайти тощо, щоб змусити людину передати необхідні дані або виконати необхідні дії.

Злочинці навіть можуть навмисно телефонувати жертві з різних номерів, щоб потім використати ці ж номери для підтвердження перевипуску sim-картки.

Як убезпечити себе

1. Будьте обережні з дзвінками від нібито представників мобільного оператора. Якщо вам телефонують із проханням надати код підтвердження або особисті дані, не передавайте інформацію та одразу завершіть розмову. У разі сумнівів самостійно зателефонуйте до свого оператора за офіційним номером.
2. Якщо підозрюєте, що вашу карту хочуть перевипустити - негайно зверніться до служби підтримки мобільного оператора. Повідомте про підозрілу активність та заблокуйте віддалений перевипуск sim-карти.
3. Перервіть “ланцюжок” шахрайських дзвінків. Якщо вам телефонують із підозрілими пропозиціями чи проханням передзвонити - відразу зателефонуйте своїм знайомим або родичам – це дозволить розірвати можливий шахрайський механізм.
4. Забороніть віддалений перевипуск sim-картки. У налаштуваннях мобільного оператора або через контактний центр можна активувати функцію, що дозволяє перевипуск sim-картки лише при особистому візиті до офіційного магазина та з пред’явленням паспорта.
5. Використовуйте унікальний номер для фінансових операцій. Бажано мати окремий номер телефону для банківських операцій, який не зазначається у відкритому доступі, зокрема в оголошеннях чи для соціальних мереж, чи месенджерів.
6. Розгляньте можливість переходу на контрактне обслуговування або прив’язку передплаченого номера телефону до паспорта. Така форма підключення забезпечує вищий рівень безпеки, оскільки перевипуск sim-карти можливий лише за особистої присутності та пред’явлення документа.

Також ви можете звернутися до свого мобільного оператора й дізнатися про інші додаткові заходи безпеки (наприклад, підтвердження зміни sim-картки через відеоверифікацію або перевірку за паспортом), і попросити увімкнути їх. Зауважте, що деякі оператори можуть стягувати додаткові кошти за подібні послуги.

Що робити, якщо стали жертвою шахраїв

- Негайно зверніться до мобільного оператора та повідомте про перевипуск sim-картки без вашого відома. Попросіть тимчасово заблокувати номер.
- При підозрі, що шахраї отримали доступ до банківського акаунту – зв’яжіться з банком та заблокуйте картки та онлайн-доступ.
- Перевірте доступ до своїх облікових записів у соціальних мережах та електронній пошті. Якщо є підозра на злам - змініть паролі.
- Якщо шахраї отримали доступ до ваших акаунтів - повідомте про це друзям та знайомим, щоб вони не потрапили у пастку шахраїв (наприклад, якщо шахраї будуть просити гроші від вашого імені).
- Зверніться до правоохоронних органів із заявою про шахрайство або подайте електронне звернення до кіберполіції за посиланням https://ticket.cyberpolice.gov.ua.

Пам’ятайте, що головна лінія захисту – ваша пильність. Дотримання базових правил безпеки може допомогти уникнути фінансових втрат та захистити приватність вашого життя.